UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/824,595	04/02/2001	Randall Scott Springfield	RPS9 2000 0016	1231

47052 7590 06/05/2008

SAWYER LAW GROUP LLP
PO BOX 51418
PALO ALTO, CA 94303

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
06/05/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@sawyerlawgroup.com
nikia@sawyerlawgroup.com

Office Action Summary	Application No.	Applicant(s)	
	09/824,595	SPRINGFIELD ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6-12 and 15-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6-12 and 15-17* is/are rejected.

7)☒ Claim(s) *6-12 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 2, 6-12, and 15-17 remain for examination. The correspondence 3/27/08 filed added claims 15-17, amended claims 1 & 6-11, and cancelled claims 3-5.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 3/27/08 has been entered.

Response to Arguments

3. Examiner disagrees with Applicant's argument that, in regards to the Grawrock invention, "the boot block identifier is untrusted, and worse, can be unscrupulous" (page 6 of the amendment of 3/27/08), given that the ultimate purpose of the Grawrock invention is to verify that the platform is trusted (col. 4, lines 35-40). Nevertheless, Applicant's arguments with respect to claims 1-17 have been considered but are moot in view of the new ground(s) of rejection, although Examiner reserves the right to reinstate rejections based upon previously cited references as may be warranted by future amendments to the claims.

Claim Objections

4. Claims 6-12 and 17 are objected to because of the following informalities: the terms “first register” and “second register” appear to be used in the claim language in a manner repugnant to their definition from the instant specification. The specification defines the first register as the register containing the identity of the actual boot source, while the second register contains the identity of the trusted boot source (page 4, lines 16-21; page 6, lines 1-11). It is unclear if the designations of "first" and "second" are simply meant to be arbitrary or if the specific sequence of registers has a significant impact on the instant invention. Claim 6 is additionally objected to because the claim further recites wherein the second register stores “an identify [sic] of the actual boot source”, which Examiner has construed as a typographic error. Appropriate correction and/or explanation is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1, 2, 6-12, and 15-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Independent claims 1 and 6 recite using registers to store one or more identities of boot sources, and then subsequently recite a comparison step between the actual boot source and the trusted boot source; however, it is unclear if the comparison step utilizes the previously recited registers by comparing the respective identities, or if in the alternative a byte-for-byte comparison of the executable code for both boot sources is made (as appears to be suggested by the "examining a location of a predetermined number of instructions" limitation). This problem is

further exacerbated in claim 1 due to the fact that the first register is disclosed as containing the trusted boot source [for which Examiner could not find support in the instant specification], whereas the second register contains *an identity* of the actual boot source, and it is not at all clear where any meaningful comparison between executable code and an identifier could be made. Claims 2, 7-12, and 15-17 are rejected by virtue of their dependency on claims 1 and 6.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claim 11 is rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claim 11 was amended to recite wherein the **first** register - which according to parent claim 6, contains the trusted boot source identity in a **write-once** register - has the identity of the actual boot source written to it **each time the computer system boots**. Clearly, the fact that the first register of the parent claim cannot by definition be re-written, coupled with the fact that the one and only write operation permitted upon it was used to store the *trusted* boot source and not the *actual* boot source as recited in claim 11, renders the claimed invention inoperable. Examiner respectfully suggests that this rejection may be overcome by amending the claim to recite wherein it is the *second* register that is operated in the recited fashion, as would be supported by the instant specification and also by common sense.

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1, 2, 6-8, 10-12, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock et al. (U.S. Patent 6,678,833) in view of Jablon et al. (U.S. Patent 5,421,006).

Regarding claim 1:

Grawrock discloses a method for verifying a boot source having a processor comprising: storing [an identity of] a boot source in a first register, the first register comprising a write-once register (col. 3, lines 63-67); determining an actual boot source used by the processor each time the computer system boots including examining a location of a predetermined number of instructions initially executed during boot up (col. 3, lines 40-60; col. 4, lines 20-35); storing an identity of an actual boot source in a second register (Ibid); and comparing the actual boot source against the trusted boot source (col. 4, lines 35-40).

Examiner submits that the Grawrock reference would, by itself, read on the claim as currently amended. However, giving Applicant the benefit of the doubt regarding the indefinite limitation of "comparing the actual boot source against the trusted boot source" (see the rejections under 35 USC 112, 2nd paragraph above), it is observed that the Grawrock disclosure is primarily focused on how one creates the identifiers by which an evaluation of whether the boot source being used is trusted, while disclosing minimal information as to exactly how the comparison is made. Thus, it is unclear whether Grawrock compares the various disclosed registers against each other. However, Jablon discloses an analogous method for verifying a trusted boot source (e.g. col. 2, lines 25-35) by comparing an identity of an actual boot source (the boot source being explicitly disclosed as being a predetermined number of instructions initially executed at boot-up: col. 11, lines 55-67) against a copy of the identity of the trusted boot source stored in write-protected memory (see the "bootCode" and "confiCode": col. 12, line 5 – col. 13, line 15). The claim is thus obvious because the technique of

comparing the identity of an actual boot source against the identity of a trusted boot source had long since been recognized as being within the ordinary capabilities of one skilled in the art.

Regarding claim 6:

Grawrock discloses a system for verifying a boot source in a computer system having a processor coupled with a boot source, comprising: a first register, comprising a write-once register, the first register for storing the identity of a trusted boot (col. 3, lines 63-67); a bridge, coupled in communication with the first register, the bridge to determine an actual boot source used by the processor each time the computer system boots including examining a location of a predetermined number of instructions initially executed boot-up (col. 3, lines 40-60; col. 4, lines 20-35; Figures 2 & 3); a second register, coupled in communication with the bridge, the second register to store an identity of the actual boot source (Ibid), wherein the bridge compares the actual boot source against the trusted boot source (col. 4, lines 35-40).

Examiner submits that the Grawrock reference would, by itself, read on the claim as currently amended. However, giving Applicant the benefit of the doubt regarding the indefinite limitation "wherein the bridge compares the actual boot source against the trusted boot source" (see the rejections under 35 USC 112, 2nd paragraph above), it is observed that the Grawrock disclosure is primarily focused on how one creates the identifiers by which an evaluation of whether the boot source being used is trusted, while disclosing minimal information as to exactly how the comparison is made. Thus, it is unclear whether Grawrock compares the various disclosed registers against each other. However, Jablon discloses an analogous method for verifying a trusted boot source (e.g. col. 2, lines 25-35) by comparing an identity of an actual boot source (the boot source being explicitly disclosed as being a predetermined number of instructions initially executed at boot-up: col. 11, lines

55-67) against a copy of the identity of the trusted boot source stored in write-protected memory (see the "bootCode" and "confiCode": col. 12, line 5 – col. 13, line 15). The claim is thus obvious because the technique of comparing the identity of an actual boot source against the identity of a trusted boot source had long since been recognized as being within the ordinary capabilities of one skilled in the art.

Regarding claims 2 and 10:

Examiner takes Official Notice that the boot sources used in the disclosed inventions would be FLASH boot sources (see the "BIOS: Definitions and Much More reference, third paragraph, and the Davis patent, col. 4, lines 40-45).

Regarding claim 7:

Grawrock further teaches wherein the computer system includes a bridge couples the processor with the actual boot source and wherein the first register and the second register are located within the bridge (col. 3, lines 7-24; Figures 2 and 3).

Referring to claim 8:

Grawrock further discloses wherein the bridge is a south bridge (the input/output control hub: element 140 of Figure 1; col. 3, lines 18-24).

Regarding claim 11:

Grawrock further discloses wherein the identity of the actual boot source is written to the first register each time the computer system boots (col. 3, lines 62-63).

Regarding claim 12:

Grawrock and Jablon further disclose wherein the processor is capable of checking the boot source stored in the first register to ensure that the boot source is the known boot source (Grawrock: col. 4, lines 35-40; Jablon: col. 12, lines 25-50).

Regarding claims 16 and 17:

Jablon further discloses shutting down the computer system responsive to the actual boot source not matching the trusted boot source (col. 13, lines 10-15).

11. Claims 9 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock in view of Jablon as applied to claims 1 & 6 above, and further in view of Davis et al. (U.S. Patent 6,401,208).

Regarding claims 9 and 15:

Neither Grawrock nor Jablon explicitly disclose wherein the trusted boot source identifier is written to the register *during the manufacture of the computer system.* However, Davis discloses an analogous method of authenticating a trusted BIOS boot source, wherein the information necessary to provide the authentication of the trusted BIOS is written into write-once memory at the time of the computer's manufacture (col. 4, lines 40-60; col. 5, lines 10-15). The claims are thus obvious because a person of ordinary skill in the art would have a good reason to pursue the known options within one's technical grasp. If writing the authentication information employed by Grawrock and/or Jablon into the write-once register at the time of the computer's manufacture would lead to success, it would likely be the product not of innovation but of ordinary skill and common sense. See *KSR v. Teleflex*, 550 U.S. at ___, 82 USPQ2d at 1397.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
5/28/08
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135